UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,232	01/31/2002	Massimiliano Antonio Poletto	12221-010001	2754

26161 7590 07/12/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,232	POLETTO ET AL.	
	Examiner	Art Unit	
	Venkatanarayanan Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *8-17,23,24,39 and 40* is/are ~~allowed.~~ objected to

6)☒ Claim(s) *1-7, 18-22, 25-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

   A person shall be entitled to a patent unless –

   (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claim 7, 21-22 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,304,262 B1 to Maloney et al.(hereinafter Maloney).

3. Regarding Claim 7, 21, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45 & Col 6 Ln 64-Col 7 Ln 6.

4. Regarding Claim 22, Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6 Ln 63-Col 7 Ln 11.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

   (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been

obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 1-6, 18-20, 22, 28-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,301,668 B1 to Gleichauf et al.(hereinafter Gleichauf) in view of U.S. Patent 6,304,262 B1 to Maloney et al.(hereinafter Maloney).

7. Regarding Claim 1, Gleichauf discloses a detection process to determine to if the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39. Gleichauf does not disclose a process of building an graph to and to classify the attack. However, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45. It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.

8. Regarding Claim 2, 3, and 4, 22, Gleichauf does not disclose a vector-based correlation process that correlates suspicious parameters and determines

existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic . However, Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6 Ln 63-Col 7 Ln 11. It would be obvious to one having ordinary skill in the art at the time of the invention to include a correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks in the invention of Gleichauf in order to a precise relationship and to differentiate between legitimate traffic as taught in Maloney see Col 7 Ln 7-11.

9. Regarding Claim 5, Gleichauf discloses the aggregate filtering see Col 1 Ln 23-31.

10. Regarding Claim 6 and 18, Gleichauf discloses the parameters including a source IP protocol, IP length, TCP/UDP ports see Col 6 Ln 24-35.

11. Regarding Claim 19, Gleichauf discloses the data collector see Fig. 2 item 36.

12. Regarding Claim 20, Gleichauf discloses the process being executed on a gateway see Fig. 2 item 20.

13. Regarding Claim 28-31 and 32, Gleichauf discloses a detection process to determine to if the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39. Gleichauf does not disclose a process of building an graph to and to classify the attack. However, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45. It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.

14. Regarding Claim 33, 34, 35, and 36, Gleichauf discloses the communicating statistics to a control center, the gateway being deployed in the network and filtering occurs on nearby routers see Fig.1 item 5, Fig. 2 item 20, Fig. 2 item 16 and 32.

15. Regarding Claim 37-38, Gleichauf discloses a detection process to determine to if the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39. Gleichauf does not disclose a process of building an graph to and to classify the attack. However,

Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45. It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful. Gleichauf does not disclose a vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic . However, Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6 Ln 63-Col 7 Ln 11. It would be obvious to one having ordinary skill in the art at the time of the invention to include a correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks in the invention of Gleichauf in order to a precise relationship and to differentiate between legitimate traffic as taught in Maloney see Col 7 Ln 7-11.

16. Claim 25 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,304,262 B1 to Maloney et al.(hereinafter Maloney) in view of U.S. Patent 6,301,668 B1 to Gleichauf et al.(hereinafter Gleichauf).

17. Regarding Claim 25, Maloney does not discloses the installing filters on routers, having data collectors, and parameters. However, Gleichauf discloses the installing of filters on routers see Col 4 Ln 33-39. Gleichauf discloses the data collector see Fig. 2 item 36. And further, Gleichauf discloses the parameters including a source IP protocol, IP length, TCP/UDP ports see Col 6 Ln 24-35. It would be obvious to one having ordinary skill in the art at the time of the invention to include installing filters on routers in the invention of Maloney in order to increase security as taught in Gleichauf see Col 4 Ln 33-39.

Allowable Subject Matter

18. Claim 8-17, 23-24, 39-40, would be allowable if rewritten ~~to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action~~ ~~and~~ to include all of the limitations of the base claim and any intervening claims.

Conclusion

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

20. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

VP
7/8/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100